UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

NATALIE WILLINGHAM, individually, and on behalf of all others similarly situated, *Plaintiff,* v. GLOBAL PAYMENTS INC., *Defendant.*	CASE NO.: 1:12-cv-01157-RWS-JFK CLASS ACTION JURY TRIAL DEMANDED

DEFENDANT GLOBAL PAYMENTS INC.'S REPLY IN SUPPORT OF MOTION TO DISMISS FIRST AMENDED COMPLAINT

Defendant Global Payments Inc. ("GP") respectfully submits this Reply In Support of Its Motion to Dismiss Plaintiffs' First Amended Complaint. As set forth more fully herein, Plaintiffs' First Amended Complaint ("FAC") does not state a single plausible claim against GP that can survive the *Twombly/Iqbal* analysis.

As a preliminary matter, Plaintiffs cannot escape the problems caused by their failure to allege any facts establishing standing, causation, and injury-in-fact. Plaintiffs argue that their claims should proceed based solely on the allegation that they incurred fraudulent charges shortly after a third-party stole data from GP. Plaintiffs have not cited a single case where a court found such sparse allegations sufficient to establish standing and to state a viable cause of action. If this Court allows Plaintiffs' claims to proceed without anything linking their alleged

fraudulent charges to the theft of data from GP, then it would be expanding liability exponentially in this jurisdiction and opening the floodgates to litigation by any consumer who alleges a fraudulent charge sometime after a data theft occurred. The Court should decline the invitation to do so.

In addition to this insurmountable obstacle, Plaintiffs' claims also fail as a matter of law because the statutes at issue – the Fair Credit Reporting Act ("FCRA"), the Stored Communications Act ("SCA"), and the Georgia Uniform Deceptive Trade Practices Act ("UDTPA") – simply do not apply to the conduct. Indeed, Plaintiffs point to no persuasive authority in support of their novel statutory interpretations. Plaintiffs' reading of these statutes implausibly stretches their plain language and grossly misinterprets their intent. More specifically:

- GP is not a "consumer reporting agency," and the information it transmits does not constitute a "consumer report," as defined by the FCRA. Moreover, GP did not violate the FCRA because it did not "furnish" a consumer report to the hackers;
- GP is neither an "Electronic Communication Service" provider nor a "Remote Computing Service" provider, one of which it must be to be liable under the SCA. GP also did not provide either service to the "public" or "knowingly divulge" any protected information as those terms are defined in the SCA;
- The Plaintiffs, non-residents of Georgia, who allege injury incurred in their respective home states, cannot state a claim under the Georgia UDTPA. Even if they could, GP made no misrepresentations regarding its services under the UDTPA, and Plaintiffs have not alleged any future harm they would allegedly suffer that the requested injunctive relief would redress.

Plaintiffs' other claims are similarly flawed. Plaintiffs assert negligence claims but are wholly unable to establish any duty flowing from GP to Plaintiffs. Plaintiffs also stretch to assert breach of contract claims even though they have no

contract with GP, are not GP customers, and have alleged no direct dealings with GP. Plaintiffs claim to be third-party beneficiaries of contracts between GP and other entities, but Plaintiffs cannot even identify the contracts at issue, much less establish that they are third-party beneficiaries of them. Plaintiffs' implied contract claim also fails as a matter of law because Plaintiffs cannot identify any statement by GP that Plaintiffs relied on, nor can they allege a relationship with GP.

Plaintiffs' failure to allege these essential elements of their claims requires dismissal of the FAC – a conclusion underscored by Plaintiffs' absolute lack of citation to analogous, recent, relevant precedent in the Response. GP's Motion to Dismiss should be granted.

I. All Of Plaintiffs' Claims Must Be Dismissed Because Plaintiffs Have Not Pled Injury-in-Fact Or Causation Sufficient To Establish Standing.

Plaintiffs' arguments that they have incurred injuries sufficient to confer standing are not supported by the governing case law, and they must be rejected. As GP established in its Motion to Dismiss, the FAC does not contain any allegations that Plaintiffs incurred pecuniary damages as a result of the GP data theft. Indeed, Plaintiffs do not even allege that they paid any money out-of-pocket or incurred any unreimbursed expenses in connection with the fraudulent charges they claim to have incurred. GP identified this fatal deficiency in its Motion to Dismiss. (Mem. in Supp. of Mot. to Dismiss at 7). Despite the devastating effect of this failure to plead on Plaintiffs' claims, Plaintiffs did not in their Response point to a single specific allegation in the FAC that establishes that they incurred pecuniary damages. This deficiency alone sounds the death knell for Plaintiffs' claims.

Plaintiffs argue they were injured by the "fraudulent purchases" on their credit cards. (Resp. at 3). But the mere fact of a fraudulent purchase does not constitute an injury. The case law in this jurisdiction is clear that reimbursed fraudulent charges to a credit card do not establish injury-in-fact. *Irwin v. RBS WorldPay, Inc.*, No. 1:09-cv-00033, at 9 (N.D. Ga. Feb. 5, 2010); *Hammond*, 2010 WL 2643307, at *8. GP pointed out in its Motion to Dismiss Plaintiffs' failure to allege that they paid any unreimbursed amounts for the fraudulent charges. (Mem. in Supp. of Mot. to Dismiss at 3-4). Plaintiffs concede this deficiency in their Response by failing to point to any allegation in the FAC where an unreimbursed payment is alleged. Plaintiffs' allegations of fraudulent charges alone are not sufficient to state an injury in fact.[1]

Plaintiffs next argue that the GP data theft put them at risk of future identify theft and fraud. (Resp. at 3). The law in this jurisdiction is clear, however, that the mere exposure of personally identifying information ("PII"), without more, does not constitute an injury-in-fact. *See RBS WorldPay*, No. 1:09-cv-00033, at 8 (N.D. Ga. Feb. 5, 2010) (Ex. A to MTD); *see also Hammond*, 2010 WL 2643307, at *8. Allegations of increased risk of future identity theft are likewise insufficient to confer standing. *See RBS WorldPay*, No. 1:09-cv-00033, at 10-11 & n.9; *Hammond*, 2010 WL 2643307, at *8; *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43-46 (3d Cir. 2011); *Allison v. Aetna, Inc.*, No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009).[2]

[1] As set forth herein at pp. 5-6, Plaintiffs also have not alleged any link between GP's conduct and these charges, as they must to establish proximate cause.

[2] Indeed, the *RBS WorldPay* court made clear that even expenses *actually incurred*

Plaintiffs rely primarily on *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) and *RBS WorldPay*, No. 1:09-cv-00033, but neither of these cases actually supports Plaintiffs' position.[3] In *AvMed*, the Eleventh Circuit allowed claims based on a data breach to proceed only when plaintiffs alleged that they were the victims of *actual* identity theft and that there was a factual basis for tying the identity theft to the defendant's data breach. Specifically, plaintiffs alleged that "the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity;" that one plaintiff's identity was stolen by changing her address; and that the other plaintiff's identity was stolen by opening an E*Trade Financial account in his name. *Id.* at 1326. These types of allegations, specifically tying the information that was compromised to the purported identity theft, are entirely absent from the FAC.

Plaintiffs *ipso facto* argue that they have alleged "actual identity theft . . .

---

to guard against future identity theft are not sufficient to show injury-in-fact. *See e.g.*, *RBS WorldPay, Inc.*, No. 1:09-cv-00033, at 10-11; *see also Hammond*, 2010 WL 2643307, at *7-8; *see also Reilly v. Ceridian Corp.*, 664 F.3d 38, 42-44 (3d Cir. 2011). Plaintiffs do not even allege that they incurred any such expenses. And, it is axiomatic that if expenses incurred to guard against future identity theft are not sufficient to establish injury, neither is the considerably more speculative risk of future identity theft without expense incurred.

[3] The remaining non-binding cases cited by Plaintiffs are also factually distinguishable. *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140-41 (9th Cir. 2010) (plaintiffs' PII had in fact been compromised; here there is no allegation that Plaintiffs' PII was compromised in the data theft); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632-34 (7th Cir. 2007) (same); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 861 (N.D. Cal. 2011) (noting that the court had "doubts about plaintiff's ultimate ability to prove his damages theory in this case"); *Arcilla v. Adidas Promotional Retail Operations, Inc.*, 488 F. Supp. 2d 965 (C.D. Cal. 2007) (not addressing standing).

directly traceable to GP's conduct," but Plaintiffs do not and cannot tie this claim back to specific allegations in the FAC.[4] For example, Plaintiffs do not even allege in the FAC that they have been the victims of identity theft. They allege "upon information and belief" that they and the putative class members suffered identity theft *or* the threat of identity theft. (FAC at ¶ 50). Likewise, Plaintiffs argue in the Response that the Heilscher Plaintiffs' receipt from alleged fraudulent purchases "showed the exact information obtained by the hackers." (Resp. at 10). But Plaintiffs do not cite a paragraph in the FAC that includes this allegation. That is because this allegation is conspicuously absent from the FAC.

Although Plaintiffs rely heavily on the *AvMed* decision, the *AvMed* Court made clear that it was not reaching the issue of whether the threat of future identity theft was sufficient to confer standing. *AvMed, Inc.*, 693 F.3d at 1323 n.1. And a threat of future identity theft is all that Plaintiffs have alleged here. The *AvMed* Court further explained that "mere temporal connection" of "time and sequence" between the data theft and the alleged fraudulent charges – exactly what Plaintiffs here allege – is not sufficient to establish the necessary causal nexus to confer standing. *Id.* at 1327. In sum, the *AvMed* decision supports GP's position – not Plaintiffs'.

---

[4] As an initial matter, Plaintiffs' accusation that GP has "kept information concerning the data breach a closely kept secret" or engaged in "negligent or deceptive withholding of information" is demonstrably false. (Resp. at 9; *id.* at n.1). As Plaintiffs' own FAC acknowledges, GP has issued numerous press releases regarding the data theft, has held an investor conference call, and has even established a website to provide relevant information about the data theft as it is uncovered. (FAC ¶¶ 29-32, 35). Plaintiffs thus bear sole responsibility for their failure to plead facts sufficient to establish standing.

Plaintiffs' reliance on *RBS WorldPay* likewise falls flat. There, this Court held that the plaintiff's "conclusory allegations" of identity theft, involving nothing more than the claim that the plaintiff had suffered an unknown charge on her credit card that had subsequently been removed by her bank, was insufficient to establish injury-in-fact. *RBS WorldPay, Inc.*, No. 1:09-cv-00033 at 8-9. The Court made clear that a party cannot adequately allege that she is a "victim of identity theft simply because she noted a charge . . . on her bank statement that was unknown to her." *Id*. Plaintiffs here allege nothing more than the plaintiff in *RBS WorldPay*, and their claims should similarly be dismissed.

II. Plaintiffs' SCA Claims Must Be Dismissed.

A. Plaintiffs fail to allege facts establishing that GP is an ECS or RCS provider.

In a futile attempt to expand application of the SCA to GP, Plaintiffs ignore the plain statutory definition of an "electronic communication service" ("ECS") and relevant precedent interpreting that definition. Binding Eleventh Circuit precedent explains that an ECS provider is a phone company, internet service provider, or electronic bulletin board system. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003). A very recent decision in the Southern District of Florida supports this proposition, dismissing the plaintiff's nearly identical allegations without leave to amend because courts have adhered to that limited definition when applying the SCA. *Burrows v. Purchasing Power LLC*, No. 1:12-cv-22800, Doc. 37 at 10, 12 (S.D. Fla. October 18, 2012) (attached as EX. A). Plaintiffs do not (and cannot) allege that GP performs one of these roles. Plaintiffs also cannot point to a single case where a payment processer, such as GP, was found to be an ECS provider in any jurisdiction.

In re Michaels also makes clear that "the provider of an electronic communication service is the *provider of the underlying service which transports the data*, such as an internet service provider or a telecommunications company whose cables and phone lines carry internet traffic, and *not the provider of a product or service which facilitates the data transport." In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 524 (N.D. Ill. 2011) (emphasis added). Applying *In re Michaels* here requires dismissal of this claim.[5] Plaintiffs do not allege that GP provided the underlying service that transports the data. GP instead provides a payment processing service which, exactly like *In re Michaels*, utilizes an internet service provider. (FAC ¶ 102). Although Plaintiffs' Response claims that GP is "analogous to the company providing the mechanism for the PIN pads to communicate to 'transaction managers, card companies, or banks,'" the SCA does not impose liability on entities that are "analogous" to an ECS provider; it imposes liability on ECS providers, and GP is not one. Moreover, Plaintiffs' argument that GP is "analogous" to the company providing ECS is directly belied by Plaintiffs' own allegations that GP is "a credit card processor . . . responsible for handling transactions when a consumer swipes a credit or debit card at a register." (*See* FAC ¶ 19, 21, 26, 36-40, 102, 104). At no point in the FAC do Plaintiffs allege that GP is the provider of the underlying internet service.

Plaintiffs also fail to establish that GP is a provider of remote computing services ("RCS"). Plaintiffs' seemingly boundless definition of an RCS would

[5] The other cases cited by Plaintiffs are similarly inapposite. *See Bohach v. City of Reno* 932 F. Supp. 1232, 1236 (D. Nev. 1996) (references criminal portion of the statute without analysis); *United States v. Weaver*, 636 F.Supp.2d 769, 769-70 (C. D. Ill. 2009) (discusses government's ability to access electronic communications with a warrant).

render every entity with computer storage an RCS. Plaintiffs allege that GP collects and stores PII, arguing that the "fact that hackers were able to obtain PII from GP's computer systems at all" qualifies GP as an RCS. By this same token, any company that has PII and is hacked would be subject to the SCA. Congress' intent, however, was to limit the scope of the SCA to companies that allow customers directly to use computing facilities in "essentially a time-sharing arrangement," meaning that the user could actually add and later retrieve data from the server for future retrieval. H.R. Rep. No. 99-647, at 23 (1986). Plaintiffs do not allege that GP provides this type of service. This alone requires dismissal of Plaintiffs' SCA claims.

B. Plaintiffs likewise fail to allege that GP provides service "to the public."

To satisfy the "public" element of the SCA, Plaintiffs rely on GP's alleged representation "to the 'community at large' that it provides services to them." (FAC at ¶¶ 25, 27). Although Plaintiffs would like to paint GP as a provider of services to the public, Plaintiffs' own complaint allegations make clear that GP acquires cardholder information through the services GP provides to "merchants, Independent Sales Organizations (ISOs), financial institutions, government agencies and multi-national corporations." (FAC at ¶ 2). In other words, the transfer and storage of transactional data from individuals is merely a by-product of the business GP engages in with merchants, credit card companies and banks.[6]

[6] The recent *Burrows* decision found that neither defendant was an ECS or RCS provider where the storage of personal information is "incidental" to the company's "main service of providing the employees with a way to purchase household goods through payroll deductions." *Burrows, No.* 1:12-cv-22800, Doc.

The definition of "public" makes it clear that this is not enough; rather, the service must be made available to "'aggregate of the citizens' or 'everybody' or 'the people at large' or 'the community at large.'" *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998). Put simply, Plaintiffs are unable to allege that the general public has the ability to send, receive and store communications with GP, and for this additional reason, their SCA claims fail.

C. Plaintiffs do not allege that the data constitute the "contents of a communication," as the SCA requires.

Plaintiffs fail to address the fact that the data that GP possesses as a result of the credit card transactions it processes does not constitute the "contents of a communication," as the SCA requires. Instead, they would have the Court believe that the SCA applies to "any transfer of signs, signals . . . data or intelligence of any nature", which is the definition of "electronic communication." 18 U.S.C. § 2510. Those same definitions specifically differentiate "contents" from "electronic communication," defining "contents" as "any information concerning the substance, purport, or meaning of that communication." In fact, the prohibitive language in the SCA that serves as the basis for Plaintiffs' claim requires that the ECS or RCS disclose "the contents of a communication" and explicitly excludes the transactional data at issue here. 18 U.S.C. § 2702; (FAC ¶ 100). In a misplaced effort to distinguish *Hill v. MCI Worldcom Commc'ns, Inc.*, 120 F. Supp. 2d 1194 (S.D. Iowa 2000) and *In re Application of U.S. for an Order Directing a Provider of Elec. Communc'n Serv. To Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), Plaintiffs argue that the holdings of these cases are limited to oral, rather

---

37 at 11-12. GP likewise *uses* an ECS to allow consumers with a way to purchase products from its merchant customers.

than electronic, communications. (Resp. at 17-18). But the SCA makes no such distinction, and these cases stand only for the proposition that transactional data, precisely the type of data at issue here, does not constitute "contents." *See, e.g., Hill*, 120 F. Supp. at 1195-96 (concluding that the "names, addresses, and phone numbers of parties . . . called" constituted "a record or other information pertaining to a subscriber or customer of such service," not contents, for a telephone account). As such, the data transferred to GP via an internet service provider is not "meaningful" communication under the SCA, such as an email or telephone conversation, but is instead transactional data that falls outside the scope of the Act.

D. Plaintiffs do not allege that GP knowingly divulged any protected communications.

Plaintiffs ask this Court to find that GP knowingly divulged protected communications because it was the victim of a third party data theft. To state this argument is to reject it. Plaintiffs make much of the fact that the SCA does not define "knowingly." (Resp. at 19). But, as set forth in GP's Motion to Dismiss, the SCA's legislative history, as well as case law interpreting the statute, make clear that there is a scienter requirement. (Mem. in Supp. of Mot. to Dismiss at 17-18). Rather than addressing this requirement (or the authorities GP cites), Plaintiffs rely on two cases that do not even mention the SCA and two loosely related definitions from Black's Law Dictionary. (Resp. at 19). Allegations that GP failed to take commercially reasonable measures to protect confidential information or failed to

notify cardholders of the data theft simply do not amount to accusations that GP knew or intended to disclose the transactional data at issue.[7]

III. Plaintiffs' FCRA Claims Must Be Dismissed.

A. Plaintiffs do not allege that GP furnished consumer information.

In yet another overly broad statutory reading, Plaintiffs allege that "GP has violated the FCRA by 'furnishing' consumer information . . . by failing to adequately secure that information leading to the entirely foreseeable theft of that information." (Resp. at 21). Plaintiffs fail to support this argument with *any* statutory analysis of the FCRA or supporting case law. In contrast, as explained in GP's opening brief, *Holmes v. Countrywide Fin. Corp.*, No. 5:08–CV–00205–R, 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012), provides a straightforward statutory interpretation of the FCRA regarding furnishing consumer reports. *Holmes* explains that "furnish" means that the alleged consumer reporting agency transmits information to another party. *Id*. Plaintiffs do not allege that GP transmitted any information to the thieves; they allege the thieves stole it. (FAC ¶¶ 5, 54, 62, 124). GP thus did not "furnish" any information (much less a consumer report) to the thieves and cannot be liable under the FCRA. Plaintiffs attempt to distinguish *Holmes* by arguing that the case involved the theft of data by an employee, not an outside party, but this is a distinction without a difference. The holding of *Holmes* remains the same; data stolen by a thief (whether that thief is an employee or an outsider) is not data transmitted or furnished by the victim of the theft.

---

[7] The *Burrows* court saw through Burrows indistinguishable attempt to stretch an allegation of failing to take "commercially reasonable measures" into knowing or intentional conduct. *Burrows*, No. 1:12-cv-22800-UU, Doc. 37 at 12.

Plaintiffs' failure to establish that GP furnished a consumer report also dooms their claim that GP violated the FCRA by failing to maintain proper safeguards. Section 1681e of the FCRA requires a consumer reporting agency to "maintain reasonable procedures . . . to limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e. Courts have consistently held that a consumer reporting agency cannot violate Section 1681e by failing to maintain reasonable procedures *unless* the consumer reporting agency also violates Section 1681b (by improperly furnishing a consumer report). *E.g.*, *Washington v. CSC Credit Servs. Inc.*, 199 F.3d 263, 266 (5th Cir. 2000). Thus, if Section 1681b has not been violated, then neither has Section 1681e. *Id.* at 267. As set forth above, GP did not furnish anything to the data thieves. And the information taken by the data thieves does not constitute a consumer report. *See* 15 U.S.C. § 1681(b), (e) (referring only to consumer reports). Under the plain language of the FCRA any security obligations only apply to consumer reports, not other information. *Id*.

B. GP does not provide consumer reports and is not a consumer reporting agency.

Continuing to try to fit a square peg into a round hole, Plaintiffs argue that GP is a consumer reporting agency providing consumer reports. Plaintiffs base this claim on two cherry-picked webpages regarding GP's Access @dvantage service.[8] These webpages refer only to services provided to merchants so they can

[8] Plaintiffs entirely failed to respond to GP's argument that they do not plausibly support their claim for willful violation of the FCRA. (*See* Mem. in Supp. of Mot. to Dismiss 21 n.4.) The Court should therefore deem Plaintiffs' willful FCRA claim abandoned and dismiss Count III on that ground alone. LR 7.1B, N.D. Ga. ("Failure to file a response shall indicate that there is no opposition to the

analyze *their own* transactions. Tellingly, neither webpage even mentions the words "credit" or "consumers," nor do the webpages state that GP assembles or evaluates consumer credit or other consumer information. In short, Plaintiffs have failed to explain how GP could be considered a consumer reporting agency providing consumer reports, meaning their unsupported allegations are not plausible and should be dismissed.

IV. Plaintiffs' Claim For Violations Of Georgia's Uniform Deceptive Trade Practices Act Must Be Dismissed.

A. Plaintiffs cannot assert a Georgia UDTPA claim.

The UDTPA is a statute sounding in tort and Georgia's *lex loci delecti* choice-of-law rule, therefore, prohibits Plaintiffs, who are out of state residents, from bringing these claims under Georgia law. *See, e.g.*, *IBM v. Kemp*, 536 S.E.2d 303, 306 (Ga. Ct. App. 2000); *Mullins v. M.G.D. Graphics Sys. Grp.*, 867 F. Supp. 1578, 1580 (N.D. Ga. 1994); *Garland v. Advanced Med. Fund, L.P. II*, 86 F. Supp. 2d 1195, 1205 (N.D. Ga. 2000) (finding that the law of Florida applied to tort claims because plaintiffs "resided at all relevant times in Florida and bore the economic impact of the alleged torts in Florida"). Instead of attempting to rebut this point with any analysis, Plaintiffs baldly state that the *lex loci delecti* rule does not apply. (Resp. at 22-23). The *lex loci delecti* rule applies to statutory claims, including the UDTPA, with full force. *Rayle Tech, Inc. v. DeKalb Swine Breeders, Inc.*, 133 F.3d 1405, 1409-10 (11th Cir. 1998) (applying Georgia's *lex loci delicti* tort choice-of-law rule to Illinois statutes). And under that rule, GP's alleged

---

motion."); *Kramer v. Gwinnett Cnty., Ga.*, 306 F. Supp. 2d 1219, 1221 (N.D. Ga. 2004) (finding claims were abandoned where party did not oppose portion of a motion).

contacts with Georgia, which arguably relate to where injury-causing conduct occurred, simply do not matter. *Mullins*, 867 F. Supp. at 1580 ("[U]nder Georgia law, the place of the wrong is where the injury was sustained and not where the last act causing the injury occurred.").

B. Plaintiffs have pled no facts to support their UDTPA claim.

Plaintiffs' Section 372(a)(5) and 372(a)(7) claims essentially allege that GP misrepresented its systems' security. Plaintiffs, however, have failed to plead any misrepresentation. Plaintiffs have alleged only that an "unauthorized third-party" hacked GP and that GP represented its systems were "hacker resistant." (FAC ¶ 5). Hacker resistant is not the same as hacker proof. If GP had meant to represent its systems were hacker proof, it could have easily said so. It did not.

Plaintiffs also fail to allege sufficient facts to support their Section 372(a)(12) claim. Plaintiffs allege that GP violated this section by "creat[ing] a likelihood of confusion or of misunderstanding by failing to notify affected customers of the nature and extent of the Data Breach, thus preventing those consumers from taking reasonable measures to protect against the threat of continued and future injury . . . ." (FAC ¶ 146). But Section 372(a)(12) does not prohibit creating a likelihood of confusion in some general sense. It only prohibits "creat[ing] confusion or misunderstanding in a manner *similar* to the conduct prohibited in subsections (a)(1) thru (a)(11) of OCGA § 10-1-372 . . . ." *Morrell v. Wellstar Health Sys., Inc.*, 633 S.E.2d 68, 73 (Ga. Ct. App. 2006) (emphasis added). Tellingly, although GP raised this issue in its Motion to Dismiss (Mem. in Supp. of Mot. to Dismiss at 29 n.11), Plaintiffs have utterly failed to explain how GP's alleged notification failure creates a *similar* likelihood of confusion. This is no oversight – Plaintiffs have not explained how its claims are similar to statutorily

prohibited conduct because they are not. Indeed, not a single provision of Section 372 even suggests GP has an affirmative duty to provide notification in a situation like the one Plaintiffs allege here.

C. Plaintiffs have failed to allege future harm warranting an injunction against GP.

To obtain an injunction under the UDTPA, Plaintiffs must establish that they are "likely to be damaged" by GP's supposed deceptive trade practice in the future. O.C.G.A. § 10-1-373 (a); *Vie v. Wachovia Bank, N.A.*, No. 1-11-CV-3620 (N.D. Ga. Apr. 6 2012); 2012 WL 1156387; *Morton v. Suntrust Mortg. Inc.*, No. 1:10-CV-2594, 2010 WL 5055822, at *7 n.14 (N.D. Ga. Nov. 5, 2010). Plaintiffs must also show that the injunction they seek will prevent future harm. *See, e.g., Vie*, 2012 WL 1156387, at *3. Plaintiffs claim that they will be harmed in the future because the thieves, who Plaintiffs allege stole their PII, could misuse their PII at some hypothetical, undetermined point. (Resp. at 26). Plaintiffs further allege that an injunction forcing GP to notify people about the alleged data breach would prevent this potential future harm. All of these allegations are based on mounds of speculation: that the Plaintiffs' PII was part of what the thieves stole; that the allegedly stolen information will be misused in the future; that notification is necessary under O.C.G.A. § 10-1-910, a legal theory Plaintiffs have failed to explain; and that an injunction would prevent the alleged future harm. Speculation about future harm is insufficient to sustain a UDTPA claim, meaning Plaintiffs' UDTPA claim fails. *See Byung Ho Cheoun v. Infinite Energy, Inc.*, 363 F. App'x 691, 695 (11th Cir. 2010) (affirming district court's dismissal of plaintiff's UDTPA claim where plaintiff alleged only "hypothetical future harm"); *Friedlander v. HMS-PEP Prods., Inc.*, 485 S.E.2d 240, 241-42 (Ga. Ct. App. 1997)

(rejecting argument that speculative future harm could support a UDTPA claim).

Plaintiffs have also failed to allege facts to show that they are "likely to be damaged" by any alleged ongoing misrepresentations. As GP argued in its opening brief, to show they are "likely to be damaged" by ongoing misrepresentations, Plaintiffs would have had to allege, at a minimum, that: (i) the alleged security flaws still exist; (ii) another breach would occur; (iii) Plaintiffs' information would be compromised as part of that breach; and (iv) Plaintiffs' information compromised in the second hypothetical breach would be different from the information allegedly compromised in the first breach. Plaintiffs call this argument specious and claim that it "completely ignore[s] the fact that Plaintiffs' and Class Members' PII has both been accessed by, and remains in the hands of, unauthorized users." (Resp. at 28). But the harm Plaintiffs assert would arise from this "fact" would be due entirely to alleged *past* misrepresentations. *Catrett v. Landmark Dodge, Inc.*, 560 S.E.2d 101, 106 (Ga. Ct. App. 2002) (noting that an injunction would not remedy a past misrepresentation). GP's alleged ongoing misrepresentations could only potentially cause Plaintiffs future harm under the circumstances outlined above.

V. Plaintiffs Fail To State A Claim For Negligence.

A. Plaintiffs' negligence claim is governed by the law of the state of residence of each Plaintiff.

Plaintiffs acknowledge that Georgia applies the *lex loci delicti* rule for torts, applying the substantive law of the state where the tort is committed. (Resp. at 29). It is well-settled under Georgia law that a tort occurs where the injury is sustained. *See, e.g., Mullins*, 867 F. Supp. at 1580. Plaintiffs' purported injuries would have occurred in their respective states of residence because that is where

Plaintiffs would have born any purported economic loss. *See Garland v. Advanced Med. Fund, L.P. II,* 86 F. Supp. 2d 1195, 1205 (N.D. Ga. 2000) (finding that the law of Florida applied to tort claims because plaintiffs "resided at all relevant times in Florida and bore the economic impact of the alleged torts in Florida").[9] Thus, Kansas law applies to Willingham's claim while California law applies to the Heilschers' claims.[10]

B. GP owes no duty of care to Plaintiffs.

Plaintiffs strain to find a legally cognizable duty owed by GP, ignoring a multitude of precedent holding that no duty of care exists in the data breach context that where, as here, there is no direct relationship between the plaintiff and the defendant. *See, e.g., Hammond*, 2010 WL 2643307, at *9; *Worix v. MedAssets, Inc.*, No. 11 C 8088, 2012 WL 1419257, at *3-6 (N.D. Ill. Apr. 24, 2012).

---

[9] Plaintiffs contend that under *Phillips Petroleum v. Shutts*, 472 U.S. 797, 836-38 (1985), the Court should apply Georgia law to this action. *Shutts* is entirely irrelevant, however, because it did not involve a tort claim similar to Plaintiffs' negligence claim, it involved Kansas's choice of law rules, and its holding was only that application of Kansas law was not constitutionally impermissible. *Id.* The remaining cases cited by Plaintiffs are similarly irrelevant. *See Franchise Tax Bd. of Cal. v. Hyatt*, 538 U.S. 488, 494-95 (2003) (discussing Nevada court's decision to apply Nevada law to a tort causing injury to a California resident in Nevada); *In re Mercedes-Benz Tele Aid Contract Litig.*, 257 F.R.D. 46, 55-58 (D.N.J. 2009) (analyzing non-Georgia choice of law rules at the class certification stage).

[10] Plaintiffs erroneously suggest that GP has argued only that that Plaintiffs have failed to allege facts sufficient to state a claim for duty, causation, and injury. (Resp. at 31). In fact, as stated in its Motion to Dismiss, GP also contends that Plaintiffs have not pled facts sufficient to allege "any duty that GP has breached." (Mem. In Supp. of Mot. to Dismiss at 31). Simply put, because Plaintiffs have not adequately pleaded a duty, they have clearly failed to adequately allege a breach of such duty.

Plaintiffs make no attempt to address these cases, instead arguing that some courts have allowed negligence claims in data breach cases to proceed. Although the *AvMed* decision did not provide any substantive analysis of the negligence claim at issue in that case, it is still readily distinguishable on the question of duty because the plaintiffs were *AvMed* customers. *AvMed, Inc.*, 2012 WL 3833035, at *1. In contrast, Plaintiffs here do not allege and cannot allege that they were GP's customers or had any direct business relationship with GP. Similarly, the Court in *RBS WorldPay* found that a plaintiff who, like Plaintiffs here, had merely alleged the existence of fraudulent charges on her credit card failed to allege sufficient injury-in-fact to establish standing, therefore, never reaching the question of duty as to that plaintiff.[11] *RBS WorldPay, Inc.*, No. 1:09-cv-00033, at 12.[12]

In a similarly futile attempt to pin a duty to GP, Plaintiffs argue that such a duty could arise under contract principles. Even if Plaintiffs had adequately alleged the existence of a contract—and they have not—Plaintiffs' negligence action would be barred by the economic loss doctrine, which provides that "a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort." *City of Cairo v. Hightower Consulting Eng'rs*, 629

[11] While the court did state that the remaining plaintiff, who had suffered actual identity theft as evidenced by specific pleadings in support thereof, had stated a claim for negligence, the court provided no substantive analysis on the issue of duty. *RBS WorldPay, Inc.*, No. 1:09-cv-00033, at 16.

[12] Plaintiffs' remaining cases are similarly unavailing on the question of duty because they involved suits by customers against the businesses to whom they provided their PII and did not even address the issue of duty in the negligence context. *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (suit by a customer of a grocery store against the grocery store); *RockYou*, 785 F. Supp. 2d at 866 (suit by users of applications against application developer to whom users had provided their PII).

S.E.2d 518, 525 (Ga. Ct. App. 2006). This rule has regularly been applied to dismiss negligence claims in data breach cases. *See AmeriFirst Bank v. TJX Cos., Inc.* (*TJX Companies Retail Sec. Breach Litig.*), 564 F.3d 489, 498 (1st Cir. 2009); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175-78 (3d Cir. 2008); *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 590 (S.D. Tex. 2011).

GP also does not have a duty to Plaintiffs under the voluntary undertaking doctrine because the doctrine is only available to a plaintiff who has suffered *physical harm* as a result of the defendant's failure to use due care in a voluntary undertaking. *See Huggins v. Aetna Cas. & Sur. Co.*, 264 S.E.2d 191, 192 (Ga. 1980) (quoting Restatement 2d Torts § 324A); *Paz v. California*, 559, 994 P.2d 975, 977 (Cal. 2000) (same); *Barber v. Williams*, 767 P.2d 1284, 1289 (1989) (same). Plaintiffs have not alleged and cannot allege that they have suffered physical harm, and the doctrine is therefore inapplicable.

Moreover, GP does not owe a duty to Plaintiffs to comply with industry standards or commercially reasonable methods to safeguard PII. *See Dupree v. Keller Indus., Inc.*, 404 S.E.2d 291, 296 (Ga. Ct. App. 1991) (holding that, while defendant had a duty to comply with federal regulations and industry safety standards, it owed no such duty to plaintiffs who were not defendant's employees). Plaintiffs cite no case law that would support a finding that commercial standards or general industry standards such as PCI-DSS would create a legal duty running from GP to Plaintiffs.

C. Plaintiffs have also failed to adequately plead the existence of a legally cognizable injury.

Plaintiffs cite *RockYou*, 785 F. Supp. 2d at 860-61 and *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126 (N.D. Cal. 2008), for the proposition that mere exposure of PII or increased risk of identity theft is a cognizable injury. (Resp. at 34). *Ruiz* pre-dated the Ninth Circuit's decision in *Krottner v. Starbucks*, 406 F. App'x 129, 131 (9th Cir. 2010), in which the court held that actual exposure of PII and increased risk of identity theft were insufficient because "[t]he mere danger of future harm, unaccompanied by present damage, will not support a negligence action." While *RockYou* was decided after *Krottner*, it does not address *Krottner*, and another court in the Northern District of California has since rejected the notion that PII has some inherent monetary value. *See In re Facebook Privacy Litig.*, C 10-02389 JW, 2011 WL 6176208, at *5 (N.D. Cal. Nov. 22, 2011) ("[T]he Court has already rejected Plaintiffs' theory that their personally identifiable information has value."). Although Plaintiffs cite *AvMed* for the proposition that "monetary loss suffered by victims of identity theft is a legally cognizable injury," (Resp. at 34), Plaintiffs fail to note that they have not alleged any unreimbursed monetary loss, which is fatal to this argument.

VI. Plaintiffs Have Failed To Adequately Plead Their Contract Claims.

A. Due to the inadequacy of Plaintiffs' allegations, it is unclear what law applies to Plaintiffs' contract claims.

Under the principle of *lex loci contractus*, which Plaintiffs acknowledge applies (Resp. at 35), contracts are governed by the law of the place where they are made unless "it appears *from the contract itself* that it is to be performed in a State other than that in which it was made." *IBM Corp. v. Kemp*, 536 S.E.2d at 307 (2000) (emphasis added and internal quotations omitted). A contract is made

wherever the "last act essential to the completion of the contract was done." *Id.* (emphasis added and internal quotations omitted). Plaintiffs' allegations are so wholly inadequate that it is impossible to determine what law properly applies.[13] Regardless of what law properly applies, however, Plaintiffs' contract claims fail.

B. Plaintiffs have failed to adequately allege that they are third-party beneficiaries of GP's contracts.

As Plaintiffs acknowledge, a third-party beneficiary claim arises only where it clearly appears from the contract that the parties intended to benefit the third-party. The third-party beneficiary claim that this Court found sufficient to state a claim in *RBS WorldPay* demonstrates the patent inadequacy of Plaintiffs' allegations here. In *RBS WorldPay*, the plaintiff specifically alleged the existence of a contract between his bank, Citizens Bank, and the defendant, RBS WorldPay, for the issuance and processing of gift cards to its customers requiring the use of commercially reasonable efforts to prevent unauthorized or unlawful access to Citizens customers' PII. *RBS WorldPay, Inc.*, No. 1:09-cv-00033-CAP, at 18. He further specifically alleged that because he was a customer of Citizens and a

[13] With respect to Plaintiffs' third-party beneficiary claim, Plaintiffs have not identified the contract or contracts under which Plaintiffs are purportedly third-party beneficiaries so it is impossible to determine where the contract was made, whether it states an alternate state for performance, or whether it includes a choice of law provision. Similarly, Plaintiffs' conclusory allegations with respect to their implied contract claim do not even specify in what state Plaintiffs purportedly used their credit cards at a merchant that uses GP as payment processor. As such, it is impossible to determine based on the pleadings where the implied contract was "made" and whether the law of Kansas, California, Georgia, or some other state should apply. Plaintiffs' simplistically assert that Georgia law applies simply because GP is headquartered there. (Resp. at 35). This is inconsistent with the rule of *lex loci contractus*.

recipient of an RBS WorldPay gift card, he was an intended third-party beneficiary of such agreement. *Id.*

In contrast, Plaintiffs have not identified the contracts under which they claim to be third-party beneficiaries, have not identified the parties to such contracts, have not identified Plaintiffs' relationship with such parties, and they make only a conclusory allegation that Plaintiffs were intended beneficiaries. (FAC ¶¶ 155, 165-166). Plaintiffs argue that these unspecified contracts "on their face" require GP to render some unspecified performance to third-party consumers, but the FAC does not contain such an allegation, and Plaintiffs even admit that they have never seen any of the purported contracts on which they base their claim. (Resp. at 37). Although GP recognizes that the precise terms of a contract may be initially unavailable to a plaintiff, Plaintiffs were required to do more that allege that an unspecified contract between unspecified parties is intended to provide unspecified benefits to virtually every credit card user in the country. *See, e.g., Pekarek v. Sunbeam Prods.*, No. 06-1026, 2006 WL 1313382, at *2 (D. Kan. May 12, 2006) (finding conclusory allegations that plaintiff was an intended third-party beneficiary of unspecified contracts between defendant and unspecified distributors insufficient to state a claim); *Sellers v. Bank of Am., Nat. Ass'n*, No. 1:11–CV–3955. 2012 WL 1853005, at *4-5 (N.D. Ga. May 21, 2012) (finding conclusory allegation that plaintiff was an intended third-party beneficiary of a contract, without more, insufficient to state a claim despite allegations specifically identifying the parties to the contract and the contract at issue).

C. Plaintiffs have failed to adequately allege the existence of an implied contract.

Plaintiffs' implied contract claim relies only on statements on GP's website

and on GP's Privacy Statement. Courts have held that broad statements of this sort do not give rise to contract claims where, as here, Plaintiffs do not allege that they read and relied upon those statements. *See, e.g.*, *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1199-00 (D.N.D. 2004); *In re Nw. Airlines Privacy Litig.*, No. Civ.04-126, 2004 WL 1278459, at *5-6 (D. Minn. June 6, 2004) (finding no binding contract where plaintiffs alleged that they relied on the privacy policy but not that they had actually read it); *Trikas v. Universal Card Servs. Corp.*, 351 F. Supp. 2d 37, 46 (E.D.N.Y. 2005) (noting that "broad statements of company policy do not generally give rise to contract claims" (internal quotations omitted)).

Plaintiffs' implied contract claim also fails because Plaintiffs have not alleged and cannot allege a direct relationship with GP, which courts in the data breach context have found is necessary to assert a claim for breach of implied contract. *See, e.g., In re Heartland Payment Sys.*, 834 F. Supp. 2d at 582; *Hammond*, 2010 WL 2643307, at *9-11; *Krottner*, 406 F. App'x at 129. The majority of the cases relied upon by Plaintiffs are thus distinguishable because they involved customers of the defendants who had provided their PII directly to the defendants.[14] *See In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 116 (D. Me. 2009), *aff'd in part and rev'd in part sub nom. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011); *AvMed, Inc.*, 2012

[14] Plaintiffs also rely on *RBS WorldPay*. Although the *RBS WorldPay* court denied a motion to dismiss an implied contract claim brought, it did so with little substantive discussion of the pleadings. *RBS WorldPay, Inc.*, No. 1:09-cv-00033-CAP, at 15. *RBS WorldPay* is distinguishable in any event because the plaintiff there had specifically alleged that he was a customer of a particular bank, which in turn provided his PII to RBS WorldPay, *Id.* at 18, whereas Plaintiffs have alleged only in the broadest possible terms that they provided their PII to an unknown merchant who in turn provided it to GP.

WL 3833035, at *3.

CONCLUSION

For the reasons stated above and on the authorities cited, GP respectfully submits that Plaintiffs' Complaint must be dismissed in its entirety.

October 22, 2012

/s/ Kristine McAlister Brown
Kristine McAlister Brown
Georgia Bar Number 480189
kristy.brown@alston.com
Stephanie B. Driggers
Georgia Bar Number 141231
stephanie.driggers@alston.com
ALSTON & BIRD LLP
1201 West Peachtree Street
Atlanta, GA 30309-3424
Telephone: 404-881-7000

Attorneys for Defendant,
Global Payments Inc.

CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 5.1(C)

I hereby certify that the foregoing **DEFENDANT GLOBAL PAYMENTS INC.'S REPLY IN SUPPORT OF MOTION TO DISMISS FIRST AMENDED COMPLAINT** has been prepared in a Times New Roman 14 point font, one of the font and point selections approved by the Court in Local Rule 5.1(C).

/s/ Kristine McAlister Brown
Kristine McAlister Brown

CERTIFICATE OF SERVICE

I hereby certify that on the 22nd day of October, 2012, a copy of the foregoing **DEFENDANT GLOBAL PAYMENTS, INC.'S REPLY IN SUPPORT OF MOTION TO DISMISS FIRST AMENDED COMPLAINT** was served via electronic filing, upon all attorneys of record, including:

Justin D. Miller, Esq.
Morgan & Morgan, P.A.
191 Peachtree Street, NE, Suite 4200
Atlanta, GA 30303-1748

J. Andrew Meyer, Esq.
Tamra Givens, Esq.
Rachel Soffin, Esq.
Morgan & Morgan, P.A.
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Scott Wm. Weinstein, Esq.
Morgan & Morgan, P.A.
12800 University Drive, Suite 600
Fort Myers, FL 33907-5337

/s/ Kristine McAlister Brown
Kristine McAlister Brown